

Contents

1	Introduction for PHY Security	1
1.1	Introduction	1
1.2	Outline	3
2	Unconditional Security Wireless Communication	5
2.1	Perfect Security Model	6
2.2	Powerful Multi-round Feedback for Build Wiretap Channel Model	7
2.2.1	Two Way Communication for Build-in Wiretap Channel	7
2.2.2	Multi-round Feedback for Build Wiretap Channel Model	9
2.3	Performance with LDPC Codes	11
2.3.1	The Threshold Property of LDPC Codes	12
2.3.2	Some Performance Results	14
2.4	Security Code	14
2.4.1	Coset Security Code	14
2.4.2	Unconditional Security Communication Model	18
2.4.3	Some Performance Results	19
2.5	Summary	22
3	MIMO Based Enhancement for Wireless Communication Security	23
3.1	MIMO Cross-Layer Secure Communication Based on STBC	24
3.1.1	Overview of Alamouti Code	24
3.1.2	Distort Signal Set Design for Security Purpose	25
3.1.3	The Action of the Legitimate Receiver	27

3.2	Security Performance Analysis	29
3.2.1	Attackers Action with Multiple Receive Antennas	29
3.2.2	Comparing the Proposed New Models with the Traditional Stream Cipher Encryption System	30
3.3	The Simulation Performance of the Proposed Method	32
3.3.1	The Performance Properties	32
3.3.2	The Secret Capacity	34
3.4	Summary	35
4	Physical Layer Assisted Authentication for Wireless Sensor Networks	37
4.1	System Model	37
4.2	Physical Channel Identification	39
4.2.1	Physical Layer Channel Response Extraction	39
4.2.2	Physical Layer Authentication Based on LRT	40
4.2.3	Physical Layer Authentication Based on SPRT	41
4.3	Physical Layer Assisted Authentication Based on PKI	42
4.3.1	Physical Layer Assisted Authentication Principle	42
4.3.2	Application Examples	43
4.4	Physical Layer Assisted Authentication Based on SCA	51
4.4.1	Physical Layer Assisted Authentication Principle	51
4.4.2	Application Examples	54
4.5	Summary	57
5	Detection of Node Clone and Sybil Attack Based on CI Approach	59
5.1	Detection Node Clone Based on Channel Identification	60
5.1.1	Network Model and Security Goals	60
5.1.2	Node Clone Detection Principle Based on CI	61
5.1.3	Determinant of Suspect Nodes	63
5.1.4	Performance Results	67
5.2	Detection Sybil Nodes Based on Channel Identification	70
5.2.1	Sybil Nodes Detection Principle Based on CI	72
5.2.2	Determinant of Suspect Nodes	73
5.2.3	Performance Results	74
5.3	Summary	78
	References	79